WHAT IS CLAIMED IS:

1. An apparatus for encryptically processing digital video data, followed by an encoding procedure to the processed digital video data with orthogonal transform to produce a coded video signal, the apparatus comprising:

a representative-value calculator to obtain a representative value of luminance data of a plurality of pixels of the digital video data for each of pixel blocks having a predetermined number of pixels, each pixel block corresponding to a unit of data subjected to the encoding procedure, as a quantized integer for each pixel block by using a specific function with the stored luminance data as a parameter;

a data rewriter to determine whether the quantized integer of the representative value for each pixel block is a multiple of a preset integer N of two or larger, and, if not, rewrite the stored luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer becomes a multiple of the integer N, whereas the stored luminance data remain unchanged if the quantized integer is a multiple of the integer N, thus encryptically processing the digital video data; and

an encoder to encode the encryptically processed digital video data with orthogonal transform to produce a coded video signal.

2. An apparatus for determining whether digital video data has been tampered with, the apparatus comprising:

a decoder to decode a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer for each pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

a representative-value calculator to obtain a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

a divider to divide the quantized integer of the second representative value by the integer N; and

a tamper detector to determine that the video data has been tampered with when remainders of division meet predetermined tamer criteria.

3. The apparatus for determining whether digital video data has been tampered with according to claim 2, wherein the division is performed for all the pixel blocks to obtain remainders, the tamper detector determining that the video data has been tampered with when at least one remainder other than zero is found among the remainders for one pixel block of the video data.

4. The apparatus for determining whether digital video data has been tampered with according to claim 2 further comprising a calculator to count the number of remainders given by the divider, the remainders corresponding to a video zone of a specific size, the tamper detector determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + B) \leq Z1$ is met, where A and B are the number of remainders zeros and other remainders, respectively, among the remainders given by the divider, and Z1 is a preset value larger than 1 / N.

5. The apparatus for determining whether digital video data has been tampered with according to claim 2, wherein the integer N is four or larger, the apparatus further comprising a calculator to count the number of remainders given by the divider, the remainders corresponding to a video zone of a specific size, the tamper detector determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + C) \leq Z2$ is met, where A is the number of remainders zeros among the remainders given by the divider and C is the number of remainders among the remainders given by the divider but each being a median from among zero to the integer N, and Z2 is a preset value larger than 1/N, the remainders to be counted as the number C being two integers most close to the integer N when the integer N is an odd number.

6. An apparatus for determining whether digital video data has been tampered with, the apparatus comprising:

a decoder to decode a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for

each of pixel blocks, as a quantized integer for each pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

a representative-value calculator to obtain a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

a divider to divide the quantized integer of the second representative value by the integer N, the division being performed for all the pixel blocks to obtain remainders; and

a tamper detector to determine that the video data has been tampered with when at least one remainder other than zero is found among the remainders for one pixel block of the video data.

7. An apparatus for determining whether digital video data has been tampered with, the apparatus comprising:

a decoder to decode a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer per pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform to produce the coded signal;

a representative-value calculator to obtain a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

a divider to divide the quantized integer of the second representative value by the integer N;

a calculator to count the number of remainders given by the divider, the remainders corresponding to a video zone of a specific size; and

a tamper detector to determine that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + B) \leq Z1$ is met, where A and B are the number of remainders zeros and other remainders, respectively, among the remainders given by the divider, and Z1 is a preset value larger than 1 / N.

8. An apparatus for determining whether digital video data has been tampered with, the apparatus comprising:

a decoder to decode a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer per pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of four or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

a representative-value calculator to obtain a second representative value of the luminance data of the decoded signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

a divider to divide the quantized integer of the second representative value by the integer N;

a calculator to count the number of remainders given by the divider, the remainders corresponding to a video zone of a specific size; and

a tamper detector to determine that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + C) \leq Z2$ is met, where A is the number of remainders zeros among the remainders given by the divider and C is the number of remainders among the remainders given by the divider but each being a median from among zero to the integer N, and Z2 is a preset value equal to or larger than 1/N, the remainders to be counted as the number C being two integers most close to the integer N when the integer N is an odd number.

9. A method of encryptically processing digital video data, followed by an encoding procedure to the processed digital video data with orthogonal transform to produce a coded video signal, the method comprising the steps of:

obtaining a representative value of luminance of a plurality of pixels of the digital video data for each of pixel blocks having a predetermined number of pixels, each pixel block corresponding to a unit of data subjected to the encoding procedure, as a quantized integer for each pixel block by using a specific function with the stored luminance data as a parameter;

determining whether the quantized integer of the representative value for each pixel block is a multiple of a preset integer N of two or larger, and, if not, rewriting the stored luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer becomes a multiple of the integer N, whereas the stored luminance data remain unchanged if the quantized integer is a multiple of the integer N, thus encryptically processing the digital video data; and

encoding the encryptically processed digital video data with orthogonal transform to produce a coded video signal.

10. A method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer for each pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the

integer N; and

determining that the video data has been tampered with when remainders of division meet predetermined tamer criteria.

11. The method of determining whether digital video data has been tampered with according to claim 10, wherein the dividing step is performed for all the pixel blocks to obtain remainders, the determination step including the step of determining that the video data has been tampered with when at least one remainder other than zero is found among the remainders for one pixel block of the video data.

12. The method of determining whether digital video data has been tampered with according to claim 10 further comprising the step of counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size, the determining step including the step of determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + B) \leq Z1$ is met, where A and B are the number of remainders zeros and other remainders, respectively, among the remainders given in the dividing step, and Z1 is a preset value larger than 1 / N.

13. The method of determining whether digital video data has been tampered with according to claim 10, wherein the integer N is four or larger, the method further comprising the step of counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size, the determining step including the step of determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + C) \leq Z2$ is met, where A is the number of remainders zeros among the remainders given in the dividing step and C is the number of remainders among the remainders given in the dividing step but each being a median from among zero to the integer N, and Z2 is a preset value larger than 1/N, the remainders to be counted as the number C being two integers most close to the integer N when the integer N is an odd number.

14. A method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel

blocks, as a quantized integer for each pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the integer N, the division being performed for all the pixel blocks to obtain remainders; and

determining that the video data has been tampered with when at least one remainder other than zero is found among the remainders for one pixel block of the video data.

15. A method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer per pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the integer N;

counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size; and

determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + B) \leq Z1$ is met, where A and B are the number of remainders zeros and other remainders, respectively, among the remainders given in the dividing step, and Z1 is a preset value larger than 1 / N.

16. A method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer per pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of four or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the integer N;

counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size; and

determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + C) \leq Z2$ is met, where A is the number of remainders zeros among the remainders given in the dividing step and C is the number of remainders among the remainders given in the dividing step but each being a median from among zero to the integer N, and Z2 is a preset value larger than 1/N, the remainders to be counted as the number C being two integers most close to the integer N when the integer N is an odd number.

17. A computer-implemented method of for encryptically processing digital

video data, followed by an encoding procedure to the processed digital video data with orthogonal transform to produce a coded video signal, the method comprising the steps of:

obtaining a representative value of luminance of a plurality of pixels of the digital video data for each of pixel blocks having a predetermined number of pixels, each pixel block corresponding to a unit of data subjected to the encoding procedure, as a quantized integer for each pixel block by using a specific function with the stored luminance data as a parameter;

determining whether the quantized integer of the representative value for each pixel block is a multiple of a preset integer N of two or larger, and, if not, rewriting the stored luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer becomes a multiple of the integer N, whereas the stored luminance data remain unchanged if the quantized integer is a multiple of the integer N, thus encryptically processing the digital video data; and

encoding the encryptically processed digital video data with orthogonal transform to produce a coded video signal.

18. A computer-implemented method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer for each pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the integer N; and

determining that the video data has been tampered with when remainders of division meet predetermined tamer criteria.

19. The computer-implemented method of determining whether digital video data has been tampered with according to claim 18, wherein the dividing step is performed for all the pixel blocks to obtain remainders, the determination step including the step of determining that the video data has been tampered with when at least one remainder other than zero is found among the remainders for one pixel block of the video data.

20. The computer-implemented method of determining whether digital video data has been tampered with according to claim 18 further comprising the step of counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size, the determining step including the step of determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + B) \leq Z1$ is met, where A and B are the number of remainders zeros and other remainders, respectively, among the remainders given in the dividing step, and Z1 is a preset value larger than 1 / N.

21. The computer-implemented method of determining whether digital video data has been tampered with according to claim 18, wherein the integer N is four or larger, the method further comprising the step of counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size, the determining step including the step of determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + C) \leq Z2$ is met, where A is the number of remainders zeros among the remainders given in the dividing step and C is the number of remainders among the remainders given in the dividing step but each being a median from among zero to the integer N, and Z2 is a preset value larger than 1/N, the remainders to be counted as the number C being two integers most close to the integer N when the integer N is an odd number.

22. A computer-implemented method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel

blocks, as a quantized integer for each pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the integer N, the division being performed for all the pixel blocks to obtain remainders; and

determining that the video data has been tampered with when at least one remainder other than zero is found among the remainders for one pixel block of the video data.

23. A computer-implemented method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer per pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of two or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the integer N;

counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size; and

determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + B) \leq Z1$ is met, where A and B are the number of remainders zeros and other remainders, respectively, among the remainders given in the dividing step, and Z1 is a preset value larger than 1 / N.

24. A computer-implemented method of determining whether digital video data has been tampered with, the method comprising the steps of:

decoding a coded video signal produced by obtaining a first representative value of luminance data of a plurality of pixels of digital video data for each of pixel blocks, as a quantized integer per pixel block by using a specific function with the luminance data as a parameter, rewriting the luminance data with a specific requirement giving the least range of change in gradation so that the quantized integer of the first representative value becomes a multiple of an integer N of four or larger, whereas the luminance data remain unchanged if the quantized integer of the first representative value is a multiple of the integer N, thus encryptically processing the digital video data, and encoding the encryptically processed digital video data with orthogonal transform for each pixel block to produce the coded signal;

obtaining a second representative value of the luminance data of the decoded video signal as a quantized integer for each pixel block by using the specific function with the luminance data as the parameter;

dividing the quantized integer of the second representative value by the integer N;

counting the number of remainders given in the dividing step, the remainders corresponding to a video zone of a specific size; and

determining that the video data has been tampered with in the video zone of the specific size when tamper criteria $A / (A + C) \leq Z2$ is met, where A is the number of remainders zeros among the remainders given in the dividing step and C is the number of remainders among the remainders given in the dividing step but each being a median from among zero to the integer N, and Z2 is a preset value larger than 1/N, the remainders to be counted as the number C being two integers most close to the integer N when the integer N is an odd number.